REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-6, 8-16, and 18-22 are currently pending, Claims 1-6, 9-16, and 19-22 having been amended. The changes and additions to the claims do not add new matter and are supported by the originally filed specification, for example, on page 30, line 5 to page 31, line 12; and Figs. 6-8.

In the outstanding Office Action, Claims 1-5, 9-15, and 19-22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier ("Applied Cryptography," Second Edition) in view of Bo Lin et al. (GB 2345229A, hereafter "Lin"); Claims 6 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kocher et al. (U.S. Pub. No. 2001/0053220A1, hereafter "Kocher"); and Claims 8 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of Lin and Kaminaga et al. (U.S. Pub. No. 2002/0124179A1, hereafter "Kaminaga").

With respect to the rejection of Claim 1 under 35 U.S.C. §103(a), Applicants respectfully submit that the amendment to Claim 1 overcomes this ground of rejection. Amended Claim 1 recites, *inter alia*,

> a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted is different than the input data to be encrypted for the other groups, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other so that performance of at least one process from one of the groups is performed at a time between processes from another one of the groups.

Applicants respectfully submit that the applied art fails to disclose or suggest at least these features of amended Claim 1.

Schneier is directed to a description of the Data Encryption Standard (DES) and combining block ciphers. In chapter 12, Schneier describes conventional DES, which includes 16 rounds in which a function which uses a key is applied on a plaintext block 16 times (see pages 270-278 of Schneier).

In chapter 15, Schneier then describes ways to combine block algorithms to get new algorithms to increase security without designing a new algorithm. In this chapter, Schneier describes Double Encryption and Triple Encryption. In Triple Encryption, a ciphertext block is operated on three times with multiple keys (see pages 357-361 of Schneier). Schneier describes different permutations of Triple Encryption based on the types of keys used (see page 360, describing Triple Encryption with Three Keys and Triple Encryption with Minimum Key). Schneier also describes different modes of Triple Encryption involving Cipher Block Chaining (CBC), such as "Inner-CBC" and "Outer-CBC" (see page 360). In the Triple Encryption described by Schneier, including both Inner-CBC and Outer-CBC modes, ***encryption is being applied to a single plaintext file*** (see page 360, for example,, where Schneier describes encrypting "the entire file" for each of the Inner-CBC and Outer-CBC modes).

The Office Action takes the position that Schneier discloses "mixing processing sequences of encryption processing units of the plurality of groups with each other," as recited in previous Claim 1. The Office Action states that this feature is taught by Schneier because "DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times." (See Office Action, at page 4). In other words, the Office Action interprets the "mixing" of the groups in Schneier to be disclosed by the existence of multiple DES processes.

The Office Action also takes the position that Schneier discloses the feature of "performance of at least one process from one group is performed at a time between processes from another one of the groups," as recited in previous Claim 1. Again, the Office Action states that this feature is taught by Schneier because "DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times." (See Office Action, at page 4).

However, amended Claim 1 recites that "a control section configured to set a mixed encryption processing sequence ***by dividing an original encryption processing sequence into a plurality of groups*** composed of one or more encryption processing units, ***each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted is different than the input data to be encrypted for the other groups***, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other so that ***performance of at least one process from one of the groups is performed at a time between processes from another one of the groups***. "

Thus, amended Claim 1 defines that an original encryption processing sequence is divided into two separate independent encryption processes which each have different input data to be encrypted, and the performance of processes of these two separate independent encryption processes are mixed together in time. On the contrary, while Schneier describes robust and complex encryption schemes such as triple encryption, for each example Schneier is still only describing an overall process which operates to encrypt ***a single inputted plaintext file***. The Office Action appears to have taken the position that Schneier describes the claimed "mixing" of previous Claim 1 because the different sub-processes involved in encrypting a single plaintext file in Schneier may be interpreted as being "mixed" together. However, Schneier never describes a method in which two separate and independent

encryption processes are mixed together in time which each have a different plaintext file as the input.

Furthermore, the Office Action never shows how Schneier discloses ***an original encryption processing sequence*** being ***divided*** into the two separate groups. While Schneier describes combining different block ciphers to form a more robust method of encrypting a file, Schneier never describes having an original encryption processing sequence which is divided to obtain two separate encryption processes to be mixed. In other words, while the Office Action asserts that an overall encryption scheme in Schneier constitutes "mixing processing sequences of encryption processing units of the plurality of groups with each other," the Office Action never shows what then constitutes the original encryption processing sequence which gets divided.

Therefore, Applicants submit that Schneier fails to disclose or suggest "a control section configured to set a mixed encryption processing sequence by dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted is different than the input data to be encrypted for the other groups, said control section mixing processing sequences of encryption processing units of the plurality of groups with each other so that performance of at least one process from one of the groups is performed at a time between processes from another one of the groups," as defined by amended Claim 1.

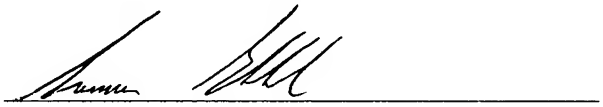
Lin, Kocher, and Kaminaga have been considered but fail to remedy this deficiency of Schneier. Thus, Applicants respectfully submit that amended Claim 1 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Amended independent Claims 9, 11, 19, 21, and 22 recite features similar to those of amended Claim 1. Thus, Applicants respectfully submit that amended Claims 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Schneier, Lin, Kocher, and Kaminaga, either alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Sameer Gokhale
Registration No. 62,618

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

I:\ATTY\SG\24'S\247305US\247305US-AM DUE 12-19-08 (MODIFIED).DOC